Discrete Mathematics 56 (1985) 133–139
North-Holland

AN EXTENSION OF THE CODES INTRODUCED BY SÉGUIN, ALLARD AND BHARGAVA

Bernard COURTEAU and Jean GOULET*

Département de mathématiques et d'informatique, Université de Sherbrooke, Sherbrooke, Québec, Canada, J1K 2R1.

Received December 1984

1. Introduction

Séguin, Allard and Bhargava [1, 4] have recently introduced a class of codes (hereafter called SAB-codes) providing error protection in byte-oriented information systems. In the case of bytes of 8 bits, these authors have proposed a 1-error correcting, 2-error detecting linear code of length 8×24 and dimension 7×23 with one parity byte which may correct any double error affecting two different information bytes.

In this paper, we define SAB-codes over any finite field GF(q) for bytes of any length l and applying some theorems in finite geometry [2, 3] we give general constructions which in the binary case and for bytes of length 8 improve the code studied in [4]. We also give a decoding algorithm based on the geometric properties of the construction.

2. Generalities

Definition 2.1. Let GF(q) be the finite field with q elements, q a power of a prime and GF$(q)^n$ the standard n-dimensional vector space over GF(q). A *partial t-spread* in GF$(q)^n$ is a set $S=\{W_i \mid i\in I\}$ consisting of t-dimensional subspaces of GF$(q)^n$ such that any non-zero vector of GF$(q)^n$ is in at most one element of S. That amounts to say that dim $W_i = t$ and $W_i \cap W_j = \{0\}$ for $i\neq j$, $i, j\in I$.

Definition 2.2. Let t be a fixed natural number and q a power of a prime. A (l, q)-byte or simply a *l-byte* is a sequence of $l \leqslant q^t$ elements in the field GF(q).

Let $S=\{W_i \mid i\in I\}$ be a partial t-spread in GF$(q)^l$. Define the $(l\times l)$ matrices M_i as follows: the first column of M_i is the zero vector and the other columns are a sequence of $l-1$ distinct non-zero vectors chosen in W_i.

* This work has supported by FCAC grant #EQ1886 and CRSNG grant #A5120.

A SAB *code with one parity l-byte over* GF(q) is then a linear code denoted SAB($M_0, \ldots, M_m, l, t, q$) defined by the following parity control matrix:

$$
H = \overbrace{\left[\begin{array}{c|c|c|c|c}
1\cdots1 & 0\cdots0 & & & \\
0\cdots0 & 1\cdots1 & & & \\
 & & \ddots & & \\
 & & & 1\cdots1 & \\
\hline
\underbrace{M_0}_{l} & \underbrace{M_1}_{l} & \cdots & \underbrace{M_m}_{l} & \underbrace{I_l}_{l}
\end{array}\right]}^{(m+2)l}
\begin{array}{l} \left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} m+1 \\ \left.\vphantom{1}\right\} l \end{array}
\qquad (1)
$$

where I_l is the identity matrix (unspecified entries are zeros).

Remark 2.3. The codewords of SAB($M_0, \ldots, M_m, l, t, q$) are thus of the form $[\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_m, \boldsymbol{b}_{m+1}]$ where $\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ are $m+1$ l-bytes called *information bytes* all of which having even parity, that is

$$\sum_{j=0}^{l-1} b_{ij} = 0, \quad i = 0, \ldots, m, \tag{2}$$

the b_{ij} being the components (in GF(q)) of $\boldsymbol{b}_i$, and where

$$\boldsymbol{b}'_{m+1} = \sum_{i=0}^{m} M_i \boldsymbol{b}'_i \tag{3}$$

is the *parity byte* ($\boldsymbol{b}'$ denotes the transpose of $\boldsymbol{b}$).

A SAB code is thus very easy to encode. His length is $(m+2)l$, his dimension $(m+1)\times(l-1)$ and his rate $(m+1)(1-1/l)/(m+2)$.

The following theorem has been proved in [1] for $q=2$ and $l=2^t$.

Theorem 2.4 (Séguin, Allard, Bhargava). *Let C be a $((m+2)l, (m+1)(l-1))$-SAB code with one parity l-byte over* GF(q). *Then C is one-error-correcting and allows to correct all double-error patterns affecting two different information bytes.*

Moreover, C is 2-error-detecting, (i) *in the binary case, when the minimum weights of the subspaces W_i are greater or equal to two, or*

(ii) *in the case $q \neq 2$, when, in addition to the preceding property, no three non-zero columns of M_i are on the same line in the affine space W_i.*

3. A geometric construction

Séguin et al. [4] considered the particular case $l=8$, $t=3$, $q=2$ and, using a computer, constructed a SAB-code with $m=23$. They wanted a code suitable for applications of byte-oriented systems, for example the ASCII format used in the Videotex system. With the aid of the following construction, we shall be able to give in this case a SAB-code with $m=30$ and to consider other interesting particular cases where for example the bytes may have 9, 11, 16 or 32 bits (in fact any l bits).

3.1. *A theorem of Beutelspacher*

Theorem 3.1 (Beutelspacher [2]). *Let $l=at+b$ where $0<b<t$. Then there exists a maximal partial t-spread S in $\mathrm{GF}(q)^l$ such that*

$$\operatorname{card} S=\sum_{i=1}^{a-1} q^{it+b}+1.$$

Proof. By induction on a, the induction step being provided by the following construction:

(1) Immerge the vector space $V=\mathrm{GF}(q)^{at+b}$ in the vector space $W=\mathrm{GF}(q)^{2[(a-1)t+b]}$ (we suppose here $a\geqslant 2$).

(2) Take a spread $S'=\{V_i \mid i=0,1,\ldots,q^{(a-1)t+b}\}$ in W where $\dim V_i=(a-1)t+b$ such that one of the V_i denoted V_* verifies $V_*\subset V\subset W$. Such a spread exists. To see this, note the identification

$$\mathrm{GF}(q)^{2[(a-1)t+b]}\equiv[\mathrm{GF}(q^{(a-1)t+b})]^2=\bar{F}^2,$$

where $\bar{F}=\mathrm{GF}(q^{(a-1)t+b})$ is the field with $q^{(a-1)t+b}$ elements and take the q-ary image (relative to a fixed base) of the line spread $D=\{L_i\}$ in the plane $\bar{F}^2$. The cardinality of D is

$$\operatorname{card} D=\frac{q^{2[(a-1)t+b]}-1}{q^{(a-1)t+b}-1}=q^{(a-1)t+b}+1.$$

(3) Take the intersection $S_1=\{V_i\cap V \mid V_i\in S'\setminus\{V_*\}\}$ of S' with V and the maximal partial t-spread S_2 in V_* such that

$$\operatorname{card} S_2=\sum_{i=1}^{a-2} q^{it+b}+1.$$

S_2 exists by the induction hypothesis because $\dim V_*=(a-1)t+b$. It is proved in [2] that $\dim(V_i\cap V)=t$ for $t\neq *$. Then we set $S=S_1\cup S_2$ and we see that

$$\operatorname{Card} S=q^{(a-1)t+b}+\sum_{i=1}^{a-2} q^{it+b}+1=\sum_{i=1}^{a-1} q^{it+b}+1. \quad \square$$

3.2. *Construction of a large class of* SAB-*codes*

We shall apply the preceding to the construction and decoding of an infinite family of SAB-codes.

Let α be a primitive element in the field $\bar{F} = \mathrm{GF}(q^{(a-1)t+b})$. Denote by $\boldsymbol{\alpha}^j$ the q-ary image (written as a column) of $\alpha^j \in \bar{F}$ relative to the natural base $\{1, \alpha, \ldots, \alpha^r\}$ (with $r = (a-1)t+b-1$) and define the product $\boldsymbol{\alpha}^i \boldsymbol{\alpha}^j$ by the equality $\boldsymbol{\alpha}^i \boldsymbol{\alpha}^j = \boldsymbol{\alpha}^{i+j}$.

Take a matrix N_0 of dimension $[l-(a-1)t+b] \times l$ with entries in $\mathrm{GF}(q)$ whose columns are all distinct, one of them being the zero vector. Such a matrix N_0 exists if $l \leqslant q^{l-(a-1)t-b}$. Noting that $l = at+b$ implies $q^{l-(a-1)t-b} = q^t$, we are assured of the existence of N_0 if $l \leqslant q^t$.

Consider the matrix

$$\bar{N}_0 = \begin{bmatrix} N_0 \\ \cdots \\ \mathrm{O} \end{bmatrix}$$

where O is the zero matrix of dimension $[2((a-1)t+b)-l] \times l$. $\bar{N}_0$ is a $[(a-1)t+b] \times l$ matrix and we have

$$\bar{N}_0 = [\boldsymbol{\alpha}^j]_{j \in J},$$

for some index set J of cardinality l. Furthermore

$$N_0 = \mathrm{trunc}\, \bar{N}_0 = [\mathrm{trunc}\, \boldsymbol{\alpha}^j]_{j \in J},$$

where trunc is a truncation operation consisting in dropping the last $2[(a-1)t+b]-l$ components of the vector to which it is applied. With these notations, we may state the following theorem.

Theorem 3.2. *Let q be a power of a prime, l and t two natural numbers such that $l \leqslant q^t$ and $l = at+b$ where $0 < b < t$ and $a \geqslant 2$.*

If α is a primitive element in the field $\bar{F} = \mathrm{GF}(q^{(a-1)t+b})$ and if the matrices are defined as above, then the partitioned matrices

$$M_i = \begin{bmatrix} \boldsymbol{\alpha}^i \bar{N}_0 \\ \cdots \\ N_0 \end{bmatrix} \quad i = 0, 1, \ldots, q^{(a-1)t+b} - 2$$

define a SAB-*code with one parity l-byte over the field* $\mathrm{GF}(q)$.

Proof. It is sufficient to apply the Beutelspacher construction as follows. The immersion $\bar{V}$ of $V = \mathrm{GF}(q)^l = \mathrm{GF}(q)^{at+b}$ in $W = \mathrm{GF}(q)^{2[(a-1)t+b]}$ is the range of the mapping

$$[x_1, \ldots, x_l] \rightarrow [x_1, \ldots, x_{(a-1)t+b}, x_{(a-1)t+b+1}, \ldots, x_l, 0, \ldots, 0].$$

The line spread $D = \{L_i\}$ in the plane $\bar{F}^2$ may be expressed as follows:

$$L_i = \{\gamma(\alpha^i, 1) \mid \gamma \in \bar{F}\} = \{(\alpha^{i+j}, \alpha^j) \mid \alpha^j \in \bar{F}\}, \quad i = 0, 1, \ldots, q^{(a-1)t+b} - 2,$$

$$L_* = \{\gamma(1, 0) \mid \gamma \in \bar{F}\} \quad \text{and} \quad L_{**} = \{\gamma(0, 1) \mid \gamma \in \bar{F}\}.$$

The q-ary image of L_i is $V_i = \{(\boldsymbol{\alpha}^{i+j}, \boldsymbol{\alpha}^j) \mid \alpha^j \in \bar{F}\}$ and its intersection with the immersion $\bar{V}$ of V in W is $W_i = V_i \cap \bar{V} = \{(\boldsymbol{\alpha}^{i+j}, \text{trunc}\, \boldsymbol{\alpha}^j) \mid \alpha^j \in \bar{F}\}$ which is a (non-maximal) partial t-spread in V. Finally, the matrix M_i is the one having $\{(\boldsymbol{\alpha}^{i+j}, \text{trunc}\, \boldsymbol{\alpha}^j) \mid j \in J\}$ as its column set. These matrices M_i for $i = 0, 1, \ldots, q^{(a-1)t+b}$ have the form indicated in the theorem. □

3.3. *Some particular cases*

We shall give examples only the binary case.

3.3.1. *Case where bytes have 8 bits*

In this case $q = 2$, $l = 8$, $t = 3$, $a = b = 2$, the field $\bar{F} = \text{GF}(q^{(a-1)t+b})$ is thus $\text{GF}(2^5)$ and the matrix $\bar{N}_0$ is

$$\bar{N}_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = [\mathbf{0}, \boldsymbol{\alpha}^2, \boldsymbol{\alpha}^3, \boldsymbol{\alpha}^{16}, \boldsymbol{\alpha}^4, \boldsymbol{\alpha}^{30}, \boldsymbol{\alpha}^{17}, \boldsymbol{\alpha}^{24}],$$

where α is a primitive element of $\text{GF}(2^5)$ such that $\alpha^5 = \alpha^3 + 1$. This case has been treated in [3]. Theorem 3.2 gives here 31 matrices M_i improving the result of [4], the partitioned nature of the matrices M_i permitting moreover an easier decoding algorithm using arithmetic in $\text{GF}(2^5)$ rather than in $\text{GF}(2^8)$.

3.3.2. *Examples where bytes have 9, 11, or 32 bits*

The interest of Theorem 3.2 lies in the fact that the byte length l may be arbitrary. To apply Theorem 3.2 it is sufficient to express l in the form $l = at + b$ with $0 < b < t$, the number $(a-1)t + b$ being the smallest possible to reduce the complexity of the arithmetic which must take place in the field $\bar{F} = \text{GF}(q^{(a-1)t+b})$. We may take $(a-1)t + b$ to be greater, if we wish to improve the rate of the corresponding SAB-code. In the case where bytes have $l = 9$ bits, we may take $t = 4$, $a = 2$ and $b = 1$. The field $\bar{F}$ is then $\text{GF}(2^5)$ and

$$\bar{N}_0 = [\mathbf{0}, \boldsymbol{\alpha}, \boldsymbol{\alpha}^2, \boldsymbol{\alpha}^{15}, \boldsymbol{\alpha}^3, \boldsymbol{\alpha}^{29}, \boldsymbol{\alpha}^{16}, \boldsymbol{\alpha}^{23}, \boldsymbol{\alpha}^4],$$

with α a primitive element of $\text{GF}(2^5)$ such that $\alpha^5 = \alpha^3 + 1$. The corresponding SAB-code has length 32×9 and dimension 31×8.

In the case where bytes $l = 11$ bits, we take $t = 4$, $a = 2$, $b = 3$. The matrix $\bar{N}_0$ is

$$\bar{N}_0 = [\mathbf{0}, \boldsymbol{\alpha}^3, \boldsymbol{\alpha}^4, \boldsymbol{\alpha}^{10}, \boldsymbol{\alpha}^5, \boldsymbol{\alpha}^{17}, \boldsymbol{\alpha}^{11}, \boldsymbol{\alpha}^{59}, \boldsymbol{\alpha}^6, \boldsymbol{\alpha}^{66}, \boldsymbol{\alpha}^{18}],$$

with α a primitive element of $\bar{F} = \text{GF}(2^7)$ such that $\alpha^7 = \alpha + 1$. The corresponding SAB-code has length 127×11 and dimension 126×10.

Finally in the case where bytes have $l = 32$ bits, we take $a = 2$, $t = 15$ and $b = 2$. The field $\bar{F}$ is then GF(2^{17}) and the matrix N_0 of dimension 15×32 admits as columns the binary representation of 32 natrual numbers between 0 and 32 768, 0 being one of these. $\bar{N}_0$ is then obtained from N_0 by adding two zero rows. If $\alpha \in \mathrm{GF}(2^{17})$ is a primitive element verifying for example $\alpha^{17} = \alpha^3 + 1$, we obtain $2^{17} - 1$ matrices of the form

$$M_i = \begin{bmatrix} \boldsymbol{\alpha}^i \bar{N}_0 \\ \cdots \\ N_0 \end{bmatrix}.$$

Different choices of a subset of these matrices will produce SAB-codes of varying length and rate, the decoding algorithm (to be given below) being the same.

4. Decoding algorithm

We shall give a decoding algorithm for any SAB-code as constructed according to Theorem 3.1.2, i.e., such that $l = at + b$, $0 < b < t$, $a \geqslant 2$, $l \leqslant q^t$, the $l \times l$ M_i matrices being of the format

$$M_i = \begin{bmatrix} \boldsymbol{\alpha}^i \bar{N}_0 \\ \cdots \\ N_0 \end{bmatrix} \quad \text{for } i \in I \subseteq \{0, 1, \ldots, q^{(a-1)t+b} - 2\},$$

where α is a primitive element of $\bar{F} = \mathrm{GF}(q^{(a-1)t+b})$ and

$$\bar{N}_0 = \begin{bmatrix} N_0 \\ \cdots \\ 0 \end{bmatrix} = [\boldsymbol{\alpha}^j]_{j \in J},$$

the $\boldsymbol{\alpha}^j$ vectors being the columns of $\bar{N}_0$. Let $m = \mathrm{card}\, I - 1$. Let $\mathbf{y} = \boldsymbol{x} + \boldsymbol{e}$ the received word where $\boldsymbol{x}$ is the transmitted codeword and $\boldsymbol{e} = [\boldsymbol{e}', \ldots, \boldsymbol{e}'_{m+1}]'$ is the error scheme.

Let us calculate the syndrome of $\mathbf{y}$. We have

$$\mathbf{s} = H_{\mathbf{y}} = H_{\boldsymbol{e}} = \begin{bmatrix} \mathbf{s}_{\mathrm{R}} \\ \cdots \\ \mathbf{s}_{\mathrm{C}} \end{bmatrix},$$

where $\mathbf{s}_{\mathrm{R}}$ and $\mathbf{s}_{\mathrm{C}}$ are known column-vectors of size $(m+1) \times 1$ and $l \times 1$, respectively.

Given the very particular structure of the M_i matrices, the column syndrome $\mathbf{s}_{\mathrm{C}}$ can be written as

$$\mathbf{s}_{\mathrm{C}} = \begin{bmatrix} \mathbf{s}_{\mathrm{C}}^{(1)} \\ \cdots \\ \mathbf{s}_{\mathrm{C}}^{(2)} \end{bmatrix} = \sum_{i \in I} M_i \boldsymbol{e}_i + \boldsymbol{e}_{m+1} = \sum_{i \in I} \begin{bmatrix} \boldsymbol{\alpha}^i \bar{N}_0 \boldsymbol{e}_i \\ \cdots \\ N_0 \boldsymbol{e}_i \end{bmatrix} + \boldsymbol{e}_{m+1}.$$

Since $(\boldsymbol{\alpha}^i \bar{N}_0)\boldsymbol{e}_i = \boldsymbol{\alpha}^i (\bar{N}_0 \boldsymbol{e}_i)$, there is no need to memorise the M_i matrices to calculate $\mathbf{s}_{\mathrm{C}}$; only $\bar{N}_0$ and the values of $\boldsymbol{\alpha}^i$ are needed.

Three cases may arise:

(A) $w(\mathbf{s}_{\mathrm{R}}) = 0$. If $w(\mathbf{s}_{\mathrm{C}}) = 0$, the received word is declared correct. If $w(\mathbf{s}_{\mathrm{C}}) = 1$,

then $\mathbf{s}_C = \mathbf{e}_{m+1}$ and we correct the error which occurred in the parity byte, in the position indicated by the non-zero component of $\mathbf{s}_C$. If $w(\mathbf{s}_C) \geq 2$, we declare an uncorrectable multiple error.

(B) $w(\mathbf{s}_R) = 1$. In such a case, we have $\mathbf{e}_i = 0$ for all $i \neq i_1$, $w(\mathbf{e}_{i_1}) = 1$, and $\mathbf{s}_{Ri_1} = e_{i_1 K} = \xi \neq 0$. If $\mathbf{s}_C^{(1)} = \boldsymbol{\alpha}^{i_1}[\mathbf{s}_C^{(2)}, 0, \ldots, 0]'$, then

$$\begin{bmatrix} \mathbf{s}_C^{(1)} \\ \cdots \\ \mathbf{s}_C^{(2)} \end{bmatrix} = \xi \begin{bmatrix} \boldsymbol{\alpha}^{i_1} \bar{N}_{0K} \\ \cdots \\ \bar{N}_{0K} \end{bmatrix},$$

and $N_{0K} = \xi^{-1}\mathbf{s}_C^{(2)}$ is the Kth column of matrix N_0. The error is corrected by subtracting ξ from the Kth component of the i_1th byte. If $\mathbf{s}_C^{(1)} \neq \boldsymbol{\alpha}^{i_1}[\mathbf{s}_C^{(2)}, 0, \ldots, 0]'$, we declare an uncorrectable multiple error.

(C) $w(\mathbf{s}_R) = 2$. In such a case, we have $\mathbf{e}_i = 0$ for all $i \neq i_1, i_2$, $i_1 \neq i_2$,

$$\mathbf{s}_{Ri_1} = e_{i_1 K_1} = \xi \neq 0 \quad \text{and} \quad \mathbf{s}_{Ri_2} = e_{i_2 K_2} = \eta \neq 0.$$

Furthermore,

$$\mathbf{s}_C = \begin{bmatrix} \mathbf{s}_C^{(1)} \\ \cdots \\ \mathbf{s}_C^{(2)} \end{bmatrix} = \xi \begin{bmatrix} \boldsymbol{\alpha}^{i_1} \bar{N}_{0K_1} \\ \cdots \\ \bar{N}_{0K_1} \end{bmatrix} + \eta \begin{bmatrix} \boldsymbol{\alpha}^{i_2} \bar{N}_{0K_2} \\ \cdots \\ \bar{N}_{0K_2} \end{bmatrix}.$$

This equality results in a linear system over the field $\bar{F} = \mathrm{GF}(q^{(a-1)t+b})$,

$$\mathbf{s}_C^{(1)} = (\xi \boldsymbol{\alpha}^{i_1})\bar{N}_{0K_1} + (\eta \boldsymbol{\alpha}^{i_2})\bar{N}_{0K_2},$$
$$\tilde{\mathbf{s}}_C^{(2)} = \xi \bar{N}_{0K_1} + \eta \bar{N}_{0K_2},$$

where $\tilde{\mathbf{s}}_C^{(2)} = [\mathbf{s}_C^{(2)}, 0, \ldots, 0]$ is the element of $\bar{F}$ obtained from $\mathbf{s}_C^{(2)}$ by concatenation of $(a-1)t + b - l$ zeros.

By resolving this system, we find

$$\bar{N}_{0K_1} = \xi^{-1}(\boldsymbol{\alpha}^{i_1} - \boldsymbol{\alpha}^{i_2})^{-1}[\mathbf{s}_C^{(1)} - \boldsymbol{\alpha}^{i_2}\tilde{\mathbf{s}}_C^{(2)}],$$
$$\bar{N}_{0K_2} = \eta^{-1}(\boldsymbol{\alpha}^{i_1} - \boldsymbol{\alpha}^{i_2})^{-1}[\boldsymbol{\alpha}^{i_1}\mathbf{s}_C^{(2)} - \mathbf{s}_C^{(1)}].$$

We then correct the 2 errors by subtracting ξ from the K_1th component of the i_1th byte and by subtracting η from the K_2th component of the i_2th byte.

References

[1] P.E. Allard, V.K. Bhargava and G. Séguin, Realization, economic and performance analysis of error-correcting codes and ARQ systems for broadcast telidon and other videotex systems Concordia Univ. Montréal, P.Q., Canada, (1981).

[2] A. Beutelspacher, Partial spreads in finite projective spaces and partial designs, Math. Z. 145 (1975) 221–229.

[3] B. Courteau and J. Goulet, Note on a class of codes introduced by Séguin, Allard and Bhargava, IEEE Trans. Comm. vol 31 (1984).

[4] G. Séguin, P.E. Allard and V. Bhargava, A class of high rate codes for byte-oriented information systems, IEEE Trans. Comm. vol. 31 (1983).